NORVIEW 2315 COVID-19 Pandemic: Response, Lessons Learned, What's Next?

Members discuss how the organization has responded to the impact to the pandemic crisis. Lessons learned on supporting WFH from a technical, hardware, security and team engagement / collaboration, and what is next perspective are shared. Polls, links, and a lively chat section are included in this April, 2020 transcript. NOREX retains the original, unedited version in order to facilitate future networking. Contact your NOREX Member Success Manager for assistance.

*Please note that this is a transcript of an audio conference and it may contain misspellings and grammatical errors. The names of participants have been abbreviated, and their organizations have been deleted from this transcript.

Previously contributed documents: 2
Supporting remote work for desktop heavy organizations 3
Poll: Personal systems accessing the corporate netword 4
Acquiring laptops, tables for this event 5
Decontaminating equipment coming back to the office 6
How to manage network and laptop password that expire during WFH 6
Ramp up vs. security 8
Creating new reports on employee status, data, supplier notifications, etc. 9
Microsoft Teams host functionality with live events 10
Ways to stimulate team connection with working remotely 13
CAD Users 14
Open forum, additional topics, what is next? 15
Poll: CV-19 Contingency Plan Working Well 18
Participant Chat Log: 19
Products/Vendors/Technologies shared in this WebForum: 28

NOREX WebForum Transcript
COVID-19 Pandemic: Response, Lessons Learned, What's Next?
April 2, 2020

Moderator: Thank you for joining this COVID-19 Response, Lessons Learned and discussion on what we foresee is next. We will begin with 80 members. In the past few weeks, we have received multiple document contributions. Our newest are linked to this transcript and available in the Pandemic Toolkit and thru search requests on the NOREX website. There are many more but the ones displayed are newly contributed from other member organizations and cleansed of their private information.

Previously contributed documents:

VIDEO MEETINGS BEST PRACTICES. Here are a few simple camera and audio tips to make your video conferencing experience successful. Specific tips on Google Hangouts are included. 1 Page (20-891)

VIDEO CONFERENCING TROUBLESHOOTING. With staff working remotely, video conference sessions are becoming a more common occurrence. Because each person's internet access at home can be different and their experience with video conferencing varies, below you'll find some troubleshooting guidance and tips.
2 Pages (20-892)

COVID-19 CONTINUITY PLAN. This plan outlines the coordinated preparation and personnel response to ensure critical services are maintained during a COVID-19 or other pandemic outbreak. 3 Pages (20-893)

EMERGENCY ONSITE & REMOTE WORK PROCEDURES. Emergency procedures for working either on site or remotely during a pandemic are described. 5 Pages (20-894)

CRISIS MANAGEMENT INTRODUCTION. Presented is an introductory plan for enabling fast and effective recovery from an unforeseen disaster or emergency which interrupts normal business operations. 28 Pages (20-895)

REMOTE VIDEOCONFERENCE BEST PRACTICES. Tips for participants and for meeting organizers while videoconferencing from remote workstations at home.
1 Page (20-896)

MEMBER ARTICLE ON REMOTE WORK IN RESPONSE TO A GLOBAL PANDEMIC. NOREX Member Mitch Planck wrote this excellent article on remote work in response to a global pandemic. Thanks for the shout-out to NOREX, Mitch!

TOPIC: Supporting remote work for desktop heavy organizations

Moderator: Richard has our first topic. How did desktop heavy organizations support remote work? Did you purchase laptops? Use home computers? Something else? How it's going and managing it, keeping track of it. What are you doing now Richard?

Richard F.: Well we used up whatever laptops we had in stock and then we actually went onto Best Buy and purchased like 10 laptops. So it's been a mix. It's been very difficult trying to get laptops from our usual suppliers at this point.

Moderator Chris, you mentioned last week that you have to purchase many laptops?

Chris Z.: Well actually purchasing laptops was kind of not an option. We had a couple of thousand on order and the orders had been delayed. What we've been doing is taking all the older laptops we have, refurbishing them and sending them out and at the same time, you know at least they have our devices. We also have a working group in place that's taking a look at other options and these options can include everything from sending a USB stick to a person with a copy of Windows 10 with our disc on it all the way up to VDIs, we have a limited VDI pool but we are now starting to use the Microsoft Virtual Desktop system up in the cloud and we've tied that to our Active Directory and so far it seems to be working pretty good. So we're going to be rolling that out to probably about 1,000 or 2,000 people in India so they can work and still have our security controls. So we're moving pretty heavily towards virtual devices whenever possible. We have a lot of laptops out in the field so that's good but for the ones that people are working from home, BYOD, virtual devices seem to be the way to go.

Moderator: Thank you Chris. Thanks for starting us off. We've got some chats going on here too.

We actually installed VPN clients, says Arthur, on our desktops and asked our users to bring them home together with their monitor, keyboard and mouse, we aren't able to get any laptops as they were not in stock.

We took training laptops we had to send those out. When we ran out of those, we started sending desktops home with people.

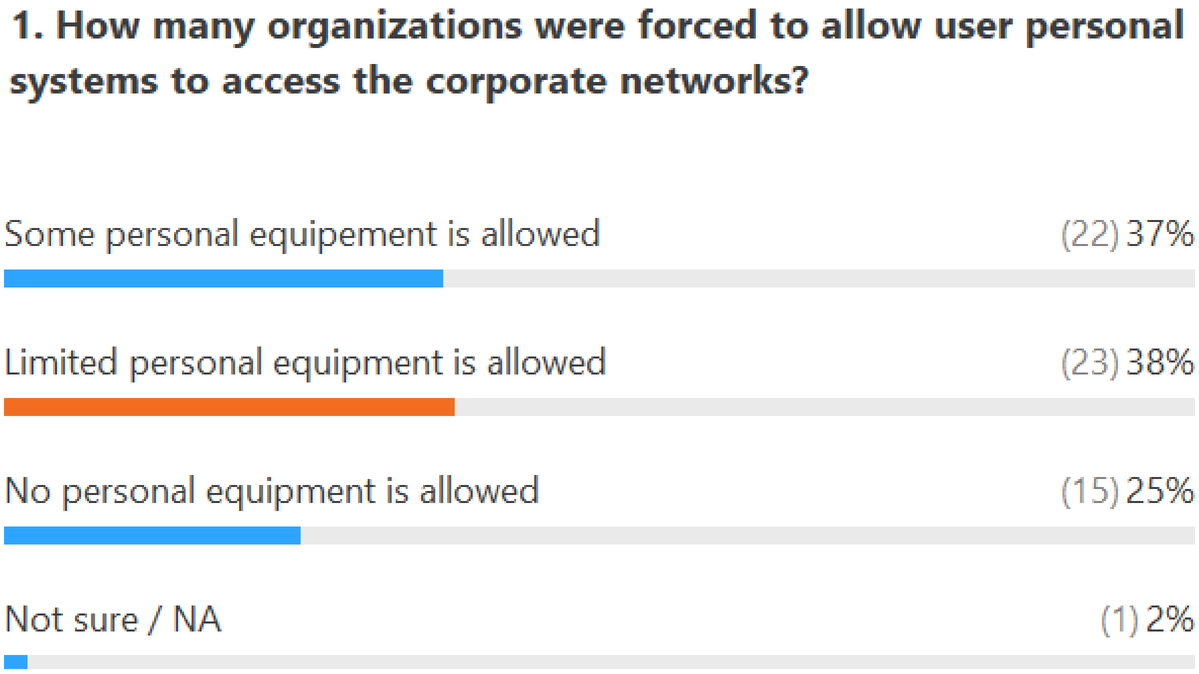
Matt A.: We've never prepared for a pandemic but we headed their disaster type scenarios and actually we have an image that we did, it, pre-started this like 10 years ago and per the chat, we had the Cisco AnyConnect part of our image so that way if someone, we'd never planned on having most of our workforce being home, but actually that tied right into this well because everyone was already prepared, we just had to set up accounts and they took their desktops home. I don't know if anybody else ran into this, but issues finding USB headsets because we use the Jabbers Softphone Client. So we ran into the USB headset problems and so what we did there is that we actually purchased some Meraki MX64's and those are deployed out with the user and they can take their Cisco physical phone home with them and we configured the ports, which you can do it all in the cloud, we configured a port where one, the computer plugs in and then a port where, these particular devices by the time we purchased these was going to purchase Meraki devices that the ones we needed didn't have POE's so we actually had to buy a NETGEAR switch also that they had to use for POE, that's actually I think the Z model that has Wi-Fi, POE and the Works all in one. But those sold out really quick before we got around to purchasing. So we're doing that with some users where they just take their PC, they take their monitor and they take their physical phone and it's like their home office now.

Moderator: Matt, thank you. Other comments and I'm sure you're reviewing the chat as well. There's too many for me to repeat them. We'll be including the chat separately in the transcript.

Richard F.: I just wanted to see if everyone was in the same boat as us and it sounds very similar to what we did also. We have a mix of things. We prefer people not use their personal computers if we can but because we have remote desktop services we've been allowing people to use their personal computers from remote desktop services and then any company type of laptop or corporate laptop, we're allowing the VPN to come through, things like that. It has been working and we've been getting it done.

Moderator: Excellent. Thanks Richard. I put up a poll. How many organizations were forced to allow user personal systems to access corporate networks?

Poll: Personal systems accessing the corporate network



1. How many organizations were forced to allow user personal systems to access the corporate networks?

Some personal equipement is allowed (22) 37%

Limited personal equipment is allowed (23) 38%

No personal equipment is allowed (15) 25%

Not sure / NA (1) 2%

Chris Z.: I think the personal device question is kind of interesting. Our big concern, you know for people with personal devices is of course, we have no way of really identifying what kind of malware detection software or what standards those devices are. So we've been restricting them. Those are not allowed to access our VPN, you know to actually get access to our network. The way they can get in, we have allowed people to connect up using the VDIs, virtual desktop interfaces and our thought is our multi-factor authentication is pretty good. So it's taking care of if they do have a key logger on their home device, etc., etc. and they get the password, they'd still be multi-factor. So we're allowing it in that circumstance and VDIs definitely seem to be the way we're going to go moving forward because they are, you know, if we can get them deployed in the cloud quickly, it will allow us to bring more and more people online as we hire and place more people around the world.

Matt A.: In regards to the personal computers, we talked about that and it's like worst case scenario if we do that and that's where that MX64 comes in, the Meraki MX64, you can configure it up in the cloud to where someone could plug their personal computer into it and you limit what it can access on your network and you can make it limit to RDP, which is like I said, it's a worst case scenario. No one's using that but that would allow them to do that because you have all those unknown factors of that person's computer, maybe they do have malware, they don't know they have it. I mean, you just don't know the environment that that personal computer but those Meraki MX64s is what we're using but I think there's a Z series that would be the better fit. But that seems to be an option.

TOPIC: Acquiring laptops, tables for this event

Moderator: The next topic is fairly similar along those same lines. Greg, how many organizations acquire laptops, tablets specific for this event versus making due with the assets on hand? If additional assets were required, what was the purchase?

Greg E.: It seems to be a common question. We ran into trying to find some additional equipment and then ultimately just decided that if you've got a desktop, you're going to have to take your desktop and a monitor home with you and we went with some USB wireless devices to get them to connect to home Wi-Fi systems and instead of allowing the home users to just use their home assets since we couldn't guarantee what was protected there. So it, I think everyone's kind of in the same boat. That seems to be a very common issue with equipment availability right now.

Moderator: Yes it does. Paul, you mentioned, we have used Microsoft RDS to limit what resources remote users have access to when they connect. We had to purchase laptops.

We were able to purchase some from CDWG says Sadie.

Stephen shares, his organization has everyone working from laptops his organization already so they just got to take all home. Home printing and scanning are still issues but mostly for people without large displays at home, who are just mentally stuck in the paper land. I have a little bit of that challenge, I had to bring my printer home.

TOPIC: Decontaminating equipment coming back to the office

Moderator: Anthony, you are wondering if there has been any discussion or documents shared regarding decontaminating laptops and the mobile phones, etc. that would be coming back to the office once all our current remote only situations have been ended? We pray for that day. Are you on Anthony? Great question in the chat, says Mike. Hopefully Anthony's on. Why don't we get some comments please?

Chris Z.: Quick comment, since my company gets a lot of laptops in we are decontaminating, wiping down and I believe we're quarantining the laptops for a couple of days before we actually touch them. Likewise, any users that do have to touch laptops are using protective gear. So we are limiting spread that way.

Moderator: Thanks Chris. And Sadie says, we've been following the CDC guidelines with a link in the chat. Thank you Sadie.

Polly says we would disinfect as part of re-provisioning process. More planning for all that of course will be coming for the future.
We've been using Teams Remote Control for IT support.

Devices should be wiped down and quarantined for at least a week, says Mark.

TOPIC: How to manage network and laptop password that expire during WFH

Moderator: David, how do IT departments handle network and laptop passwords that expire or need reset soon while at work from home? We currently need the employees to come on site to connect to the network so that their domain joined laptop and network passwords are properly synced. While the employees can change their network password, their laptops won't recognize it and they will have two passwords. David, are you on?

David C.: Yes, that lays it out. We're having issue and we're going to come up across more people who are working remotely, their passwords will expire, you can't just change it because that policy is on the laptops. So if anybody else is up against this problem, what are you doing?

Moderator: Sadie shares for you David, we stopped password expiration for people that change their password remotely. We have them connect to VPN then lock their computer, then log back in with the new password.

Sharon says, we are scheduling time for the employee to come on site to reset their password.

David C.: OK.

Moderator: In chat, extended password expiration seems to be brought up.

Richard F.: That's what we did. We just extended the password expiration for people so that they could do it. We have Office 365 and we allow passwords to be changed through Office 365 but you're right, the laptop doesn't recognize it so we've just been extending it for some people.

David C.: OK.

Moderator: And Mark, it looks like it's not an issue for you as long as our users are VPN then they can do it themselves and stay synced?

Mark M.: Yes and I was just commenting on that, that I also, I actually had that experience last week and reached out to my infrastructure lead. As long as I was on VPN from home I was able to lock my computer and change my password without issue.

Moderator: Stephen shares, password changes must be done over VPN. Also we are in the middle of extending our password policies to match the new NIST guidelines. At worst, it is lock and unlock screen issue. NIST guidelines, is that the passphrases Stephen or others?

Stephen T.: Correct. The longer passphrases and the less frequent expirations. Our model is you need to, their password expires when something horrible happens or just often enough that you remember how to change it when you need to.

Moderator: Thank you Stephen. Azure Active Directory connect with password write back is an option for O365 hybrid users, says Cory. Great chat today folks.

David C.: I like Kevin's comment there. Just have them live with two passwords and we're looking at that option as well.

Chadd B.: What we do, previously part of our password management tools that we have, it sends email alerts indicates that their passwords expiring in 14 days and they get an email alert until they change that password. With that on, we've not seen an issue. They can get that email and their on the VPN, they change their password and it syncs back. We also in that email included directions for them, how to change it through a web tool so that they could log in and change it there and while they're on the VPN, we've not seen issues. The laptops are picking it up okay as long as they obey that email that they get that they have 14 days and it counts down. We only see issues when they wait until it's expired.

Moderator: Thank you Chadd. Great stuff David. Anything more here?

David C.: No, that's it. Thanks very much everybody.

TOPIC: Ramp up vs. security

Oleg C.: We're actually fully deployed on Teams and whatnot but I know for us our big push was to try to get the number of call centers representatives we had quickly on remote capabilities. We had all the technologies in place but we didn't have like necessarily the capacity proof and getting Teams rolled out to the entire enterprise hadn't happened yet. So we did all that in about a couple weeks but from a security standpoint, didn't have time to really review all the different components. As an example, in Teams, the PHI, PII controls were not all there in the standard package. So we're having to now go investigate what add-ons we have. We have been able to put those in place prior to needing to get these deployed out. So I was curious if anyone else had that experience where you had to essentially assume additional risk in the short term in order to avail yourself of getting everybody remotely connected into your company's network.

Moderator: Mike, you have in the chat, HIPAA has relaxed. Anything more there Mike? Pretty quiet.

Oleg C.: Yes. It's a deep topic. I think that also depends on what you can and can't do in terms of your current organization or if anyone's really looked at it. I know for us, our security teams are basically trying to wave the flag saying hey, wait a minute, like for example, you can post PHI in a meeting chat and it doesn't get caught by anything as an example. So the question is for management, what level of risk are you ready to assume in case this happens? And I'll be blunt, no one really wants to hear about it. They just want this stuff deployed right now for a remote purpose so the business keeps going and we're a healthcare company. So that's a concern for us and we're backtracking now and we've found a solution and we're going to be implementing it but in the interim, we've had three weeks now where we didn't have that in place. I was just curious if anyone else like understood risks or at least addressed it with their management anything like that.

Chris Z.: Yes, Oleg, risk is tricky and when this thing first started picking up, one of the immediate things information security did was create a triage system so that we would start looking at all their exceptions and all the requests that may come in, triage them, identify the risks and then make informed decisions as to whether or not we wish to accept the risk. Or whether or not we could accept the risk based on our contractual agreements with all the other companies that we work with. That has been extremely helpful. To be quite honest, it's an Excel spreadsheet that we've built out into a full database at this point. But it's allowing us to say, OK, you want to stop doing this, you know, say we want to suspend patches, well that's a very high risk item and we still can do patching with the tools that we have but we recommend you keep doing that. In your case, you've got a, you know, the executive staff in your organization needs to be presented with, people are unable to communicate and their not able to do their job. This will have the additional risk in terms of PII, PHI disclosure, mitigating steps we can do is inform everyone not to post anything that may be of the PII nature, short termed training and we're building a solution, you know, to incorporate this into our DLP system.

Teams is in our DLP system right now so we're in good shape. But that said, people do have to listen to the risks and accept them or if they can't accept the risks, say no, we cannot do this. So I don't know if you have a risk register set up right now or if you have an emergency risk register handling just these specific changes but try to run them through your change management risk boards as much as possible and make informed decisions based on your company's tolerance and your company's ability to function would be my recommendation.

Oleg C.: OK. Thank you.

Chris Z.: But definitely setting up that initial requirements thing and telling all the architects and everybody else, hey, if you want the security exception and so forth, this is the emergency security exception system. We'll take a look at it and we will rank and review it as quickly as possible. That helped a lot the first week.

Moderator: Other chats here too. Mike had said, HIPAA has relaxed for the reasons of the pandemic and we are doing a lot with EMRs and nursing homes across the country. Everyone is understanding the risks are higher. And Robert, we were able to not relax any risk. We did have to delay new security steps we were about to roll out.

Oleg C.: That's good. Thank you.

TOPIC: Creating new reports on employee status, data, supplier notifications, etc.

Moderator: Mark's topic. We've had to create new reports data such as who was absent today, essential supplier notifications, etc. What other types of reporting have others been creating in response to the novel corona virus? New reports, how do you keep track of absenteeism, things you need to get to suppliers, notifications?

Mark M.: We've had to create some automated reports to get sent to our supervisors and notify them if somebody doesn't clock in for the day and they were expected to and then other things such as identifying who, which suppliers are essential to our business and moving forward and kind of give them the get out of jail free card so to speak letter. So I guess I was just looking to see if not so much if anybody's had to do those type of things, you know, those specific things but any other things that maybe we should stay on top of or we could be doing to stay ahead of the curve or get in front of it or react to it.

Moderator: Sure. Some chats here for you. David says, nothing for new hire going on.

And Paul, we are doing a daily report on connected users.

Robert, tracking who has been sent home with suspected COVID-19 at our communities.

Mike says, we have been keeping track of time which is being used for the COVID-19 tasks

How about for supplier notifications? Anything different happening or efficiencies you've followed when you're remote?

Chris Z.: Just on speaking of suppliers, we have definitely sent out updates to all of our financial people and also ensuring that they are following our processes for bank account transfers, wire transfers and anything else to vendors. Even if the vendor contacts us from their email address and says, hi, we'd like to change our bank number or something like that, we are requiring personal follow up calls from our database. We are not trusting any emails coming from vendors at this point. Because to be honest, they can get hacked and when they're hacked and then they ask us to change the routing number, if we change the routing number, we send it to the wrong address, which is sad. So it's a standard thing that we always do but when this virus or when this pandemic came out, we restarted the training for all the people that handle those kind of things and it is very clear to follow that process.

Mark M.: Awesome. That's a good idea. Thank you.

Chris Z.: Oh yes.

Moderator: Mark, Chris has got on his LinkedIn if you follow him, he's got some good pieces you've created that speak to this sort of thing.

In the chat, we are telling our suppliers to expect delayed payments and we reached out to suppliers to verify support level, says Paul.

We've been reminding users to be extra cautious and cyber aware while working from home.

Donna says, some of our facilities contacted the suppliers that they use the most individually.

In terms of associate's time entry, we modified our in-house time reporting tools to account for FFCRA legislation. What type of in-house time reporting do you use Cory? Home grown, chats Cory.

Mark M.: No, I guess I wasn't specifically looking for supplier related things or absent related things, just like any reports in general. I appreciate the help. Thank you and I will look at Chris' LinkedIn.

<u>TOPIC: Microsoft Teams host functionality with live events</u>

Moderator: Matt shares; I found Microsoft Teams live events to be lacking in host functionality. Are there upgrades that will improve it? We would like to hear more on what you are experiencing Matt? Is everyone using Zoom for live events or what Teams and other solutions offer?

We use Google Meets. I would like to be able to use Teams Live Event soon. It would be good to hear some experiences. We are using a product called BlueJeans. We hear about that.

We use Google Hangouts mostly, says Donna.

Teams is a lot better than it was six plus months ago. Teams is working good so far for them. Mostly Teams and some Zoom. Matt, please share what you felt was lacking.

Matt A.: I am curious on that. What is lacking on the host functionality because we just rolled out Office 365 fourth quarter of 2019 and Teams was not rolled out. We did a quick roll out of it because we wanted the chat feature of it. We haven't had any issues with using the host functionality. That is how our departments are having departmental meetings. We haven't had any issues with using the host functionality because that is how our departments are having departmental meetings, either every other day or some of them are having them every day using that functionality. I haven't heard anything bad on that so I would be curious as to what is lacking.

Moderator: I don't know if the other Matt is on unfortunately.

Mark M.: We are currently using Skype for Business still and we have been looking into Teams but one thing that we aren't aware of if it is out there that we think it is lacking is the ability to have it be a full call center and be able to transfer calls and do things of that nature. I don't know if there is an add on or something for it. That is one thing that has been lacking for us. We do everything on prem and we are concerned about the cloud environment for that part.

Moderator: Thank you Mark. A lot in the chat here on some Zoom security thoughts and maybe a hack that Zoom had allowing in some users.

Chadd B.: Some individual users had Zoom and then when this whole thing came up, this pandemic stuff we moved more people over to Teams and we have seen a huge increase in people having Teams meetings. The live webinar type stuff with customer, we use the Zoom webinar feature. We had that before we started using Teams and before this COVID-19 stuff. I think the Zoom webinar just has some more features for the live stuff it is a better platform in our opinion.

Matt A.: In regards to Teams I just want to clarify, we are just using it internally so we are not communicating outside the company, plus since we have an E3 license with Microsoft 365 it just made sense that we would take advantage of something that we are already paying for.

Moderator: Great comments. Thank you. Steven says the bigger issues are actually the quality and lack of transparency from Zoom about office security issues.

GoToMeeting is used, a lot of different things, different solutions used here.

Live events is really the issue mainly, live like we are on a live one now. Just looking at that Zoom alert, hopefully everyone is blocking SMV and CIFS from internal and to the internet by default. MFA is nice if you have MFA.

Chris Z.: Oh yes!

Moderator: So Chris, for our call today tell us what you think. We are on the Zoom video conferencing. We have corporate video conferencing.

Chris Z.: I just tool a quick look at the Zoom error. It looks like what somebody can do is post a link that is actually a file share and when you click on that link in chat or something like that it would attempt, your PC would happily go over and attempt to connect to their server using your encrypted credentials. SMB is not a very secure encryption system, especially if you haven't disabled SMB v1 and if possible they could reverse engineer your password.

Blocks right off the bat are totally disabling SMB v1 in your network. The second thing rest make sure that you do not allow people on your inside network to be able to connect out to the SMB hosts on the internet. The problem with that is of course now everybody’s working remote and unless your VPN routes all traffic through your company it will happily route that traffic out to that site because people at home don't have those sorts of blocks. That could be a problem.

Chadd B: So Zoom has acknowledged those and they have put a freeze on development for 90-days to fix their security blunders but the other thing, this isn't just an issue with Zoom. There is a group policy, a very easy group policy setting to block Windows from sending NTLM hashes out of your network. There is a very easy group policy. It is one setting that you can enable and it will prevent that, not just for Zoom but potential other attacks or some other service that turns network paths into links where the NTLM hashes will be sent. We have that group policy turned on and that prevents that Zoom issue. So if you are using Zoom and are worried about that if you are not blocking public SMB, that group policy is an easy thing to implement to fix that.

Man: Good idea.

Moderator: Sounds like a great tip.

Chadd B.: I will put it in the chat for everybody to see the exact fix.

Moderator: Chadd, outstanding, thank you.

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-outgoing-ntlm-traffic-to-remote-servers

Chadd B. That's the GPO fix for the HTML Hash issue

TOPIC: Ways to stimulate team connection with working remotely

Moderator: Chris, I believe, is on. What specific actions have others taken to maintain a strong sense of team and togetherness while everyone is working remotely?

Lee says, besides the Skype, Zoom meetings, team chats etc. What else are you doing to get that team connection happening.

Chris M.: I have heard others have tried to do some virtual happy hour or cocktail hour kinds of things to kind of keep people connected and together. I am just looking for other ideas to help with morale for an organization that typically is in the office together verses highly remote.

Chris Z.: I found for the security managers and so forth we are all having virtual lunches twice a week. As a matter of fact we had one today, Tuesday and Thursday at noon. We just get together, turn on our cameras and eat food. It is kind of funny of course because you have no idea what people are bringing or whatever but it does allow us just to talk about other things besides work for an hour or 30 minutes or however long somebody can be in. It has done a lot to kind of help keep us together. The little virtual lunch, come as you can, just eat food and we can all watch each other eat. It's better than meeting, meeting, meeting, meeting, meeting. So that has been helpful.

Chris M.: I will use that.

David D. One of the things that my team has been doing is we have actually got an open meeting where anyone who needs tech support can jump in. My entire team just kind of sits on there and we randomly chat and we jump out to help individuals but just having that open for the team where we are constantly in and able to interact quickly with each other, I feel, has made a big difference as well.

Moderator: Send an email every afternoon with something lighthearted, says Sharon.

A stretching session, virtual happy hour.

Mike M.: One thing that we did was for recognition when a team has kind of gone above and beyond, we have sent out delivery of an edible treat. I am not sure exactly what the treat is because my team is the recipient of one but we actually haven't received it yet but it is a thing, right. It is like hey, everybody has gone above and beyond, like on my team getting everyone to be able to work remotely from home. So management said yes, lets send them a goodie. Like I said I wish I knew what was coming but I don't.

Chris M.: I thought about doing that back to the lunch idea. I was going to send everybody pizza and then say all right, now let's eat. So kind of using that, having something delivered. I hadn't thought about just having a scheduled lunch all of the time. That would be a great idea too.

Moderator: Great idea. Dave says; our treat has been hot premade family meal delivery. One less thing to worry about for working parents.

We have got some good security related conversation going on. Security and auditing etc. in the chat.

<u>TOPIC: CAD Users</u>

Moderator: Jay asked, any thoughts on CAD users? So using CAD tools that are very heavy on bandwidth, things like that?

Chris Z.: I don't have any direct advice but we do have EZ (?) which does CAD cam work. Talk to me about it after the meeting. I will see if I can find some help for you.

Jay G.: We are just looking for ways to work with CAD people that have very high graphics intensive applications. They are hard to work over. We have done most of our remote users using RDP and so they don't work real well in RDP but sending computers home also makes a challenge, networking, getting connected to the router and things like that. Sharing files and all of those types of things make it very challenging for users. Opening files remotely takes a long time, especially like Solid Words files or all of the CAD files.

Moderator: Our CAD users are going into the office. RDP sort of works but requires some local security policies that have changed says Matt.

We have our CAD using our VDI as a jump platform to get to their desktops which are still in the office. Kevin, thank you. Autodesk makes the AutoCAD product. So you have been able to use, they have been working from home with Autodesk, Kevin?

Autodesk has sent emails to customers with some extended home use options.

RDP to the desktop in the office for AutoCAD for Chadd. Any final comments or anything else? We have got a big link that just hit the chat. Excellent. Extended access program for AutoCAD Thanks Kevin.

TOPIC: Open forum, additional topics, what is next?

Moderator: We have now covered the submitted topics. Let's make it an open forum for those who would like to talk about some lessons learned. If you change direction in a certain way, now that we are a few days or even over a week or more into a big work from home move. What is next? What is on the horizon as we take it day by day?

Matt A.: One of the things that senior management here has been talking about is that we are looking at this as a learning experience. We have learned a lot from this and we think there are going to be things that are going to come out of this being stronger. It has tested some things.

We are a 24x7 shop so from a testing standpoint it is really hard. We can't just shut down stuff. There are always trucks rolling and there is always something going on. This has allowed us to test things on the fly and so far things have been successful. They have been bumpy but we believe that this is a great opportunity to take and be stronger from a continuity and disaster scenario. So that is one of the things that we are talking about. There will be, I'm sure, a bigger meeting when we all come back together but that is kind of the chatter among all of the senior management here.

Moderator: Good point, Matt.

Chris Z.: I guess I think the question really is how long is this going to be going on? Right now I see a lot of people, we are three weeks into this for our organization at least and a lot of people are doing things still as if they were in the office. We still have our standard meetings. Everybody sits in front of the camera. We dress relatively well, which is good. I am sitting in a hammock but that is life.

That said I guess the big question is at what point does this stop being a short term thing and start being a longer term? This is how the company is going to be operating for several months or permanent. What kinds of changes are people thinking?

I am thinking of this from a security standpoint but just in terms of business operations if this keeps going on these methods that we have used in the past, do we still want to keep them? Do we want to start replacing them with new remote methods? How do we want to go forward in the long term since this isn't just a snowstorm?

Matt A.: One of the things that came out of this is that we have always had some people resistant to technology. This has forced their hand. Everyone is having to embrace it and actually the interesting thing, it doesn't really touch on the security side of it but the interesting thing is that those that have resisted it have been the ones that have embraced it and really like it. Everyone is too busy. They don't have time to use that new technology but this has forced the issue. One of the things that we still have a challenge with is that we still have people that love printing everything they get.

Chris Z.: They are going to run out of paper soon!

Matt A: What is interesting is no one can print now so it is really making them think outside the box. We gave them multiple monitors, who thought at that time back in the day was you shouldn't have to print. Just pull it up on another screen. The whole idea before was they would print it and they would set it there so that they could see it. So it is moving some people's cheese and some of them are actually embracing it but I still think that going back to what you are saying if we stay like this here we are having to figure out how to still make some of those things work such as there is a need for some printing. From a security standpoint that is a good question. I don't know.

Chris Z.: It is a thought that is starting to pile into my head. I will probably be writing on it in the next couple of weeks. It is interesting because somebody just said; we are tracking hours. This is a good question. How do you measure productivity? Are you measuring it just based off butt in a seat so to speak, time in front of the computer or tasks that need to be done? Would we shift from a strictly time based type system to a task based system? What does that do for people that are classified as hourly workers who technically have to be paid and operate on an hourly basis with overtime and everything else? These are the kinds of questions that I am looking at and going OK we are still trying to be like we were in the office because that will have to change soon. It gets weird.

Oleg C.: I was going to add to Chris' point, another think to look at is not simply how we measure productivity but at least at our organization what has become apparent is this unannounced practice now that well you are working from home so if I schedule a meeting at 5:00 or at 6:00 because you are already there, you are not traveling, or at lunchtime or if I ask you for something the next day because I have you captive.

Even though you are remote, you are always tied into the network and the users and the tasks. So that boundary of work hours verses non-work hours has really stretched beyond the norm that we had when we were still in person even though we had the ability to connect remotely all of the time.

What I have noticed, at least in our organization, is that those social barriers are kind of coming down because people are saying; you are not driving and you are still available and I can get you on Teams on your phone or on your desktop, either way. So I can contact you any time day or night.

Chris Z.: Oh dear!

Oleg C.: I don't know if other organizations are experiencing that but I have noticed that trickle happening. It is not a really huge movement but I have noticed that more and more the demand to get things done faster has increased significantly mainly because they are saying; well you are not doing anything anyway. You are sitting in front of your computer all day.

Richard F.: Yes, we have definitely noticed that quite a bit. We have had to reiterate core hours and what that means and when it is appropriate to contact people and things like that. It hasn't been crazy but it has been one of those things where we are getting calls. It just bleeds later and later into the day to 7:00 PM, 8:00 PM, 3:00 or 4:00 in the morning because there are some extreme early birds here. So we have just been kind of reiterating what the core hours are and what that means and how to get in touch with us otherwise.

Moderator: The chat is jam packed with information on this too. Good discussion. Setting boundaries is mentioned.

Using certain tools to track productivity. Toggles are mentioned and there was ManageEngine with tickets was mentioned.

Tips and tricks, Clint, you mentioned that. Once this is over I think we are going to see a lot more people wanting to work from home regularly and it will harder for us to say no.

You need to be in the office to be effective. So yes, a lot to come as we continue to work through this.

David D.: I actually really appreciated the fact that this has forced some of the things that we have been discussing have come to light. For example the topic now that we are discussing, we have mentioned this over the years that we have to have boundaries and no one has really wanted to set it however now that we are here the heads have actually been in a place to say yes, we have to enforce this to protect our employees so we have to have some of these boundaries. Where they were very reluctant to do that in the past. Again we are a school so even purely forcing our teachers to become more tech savvy has been fantastic. This has done more for our tech department than we could have achieved on our own, as sad as that is.

Moderator: Thanks David. You also shared you are guessing it could be at least another three months and possibly going back to working from home in the fall.

David D.: We are having a lot of discussions with schools around the world because our community is quite tight like that. Seeing what is happening in these other countries and how long it is taking them to get back. It has been interesting. They have all said very similar things. Oh it is only going to be two weeks. Oh no, it is a month. So we seem to be behind them and that is where my predictions are coming from.

Moderator: Great points David.

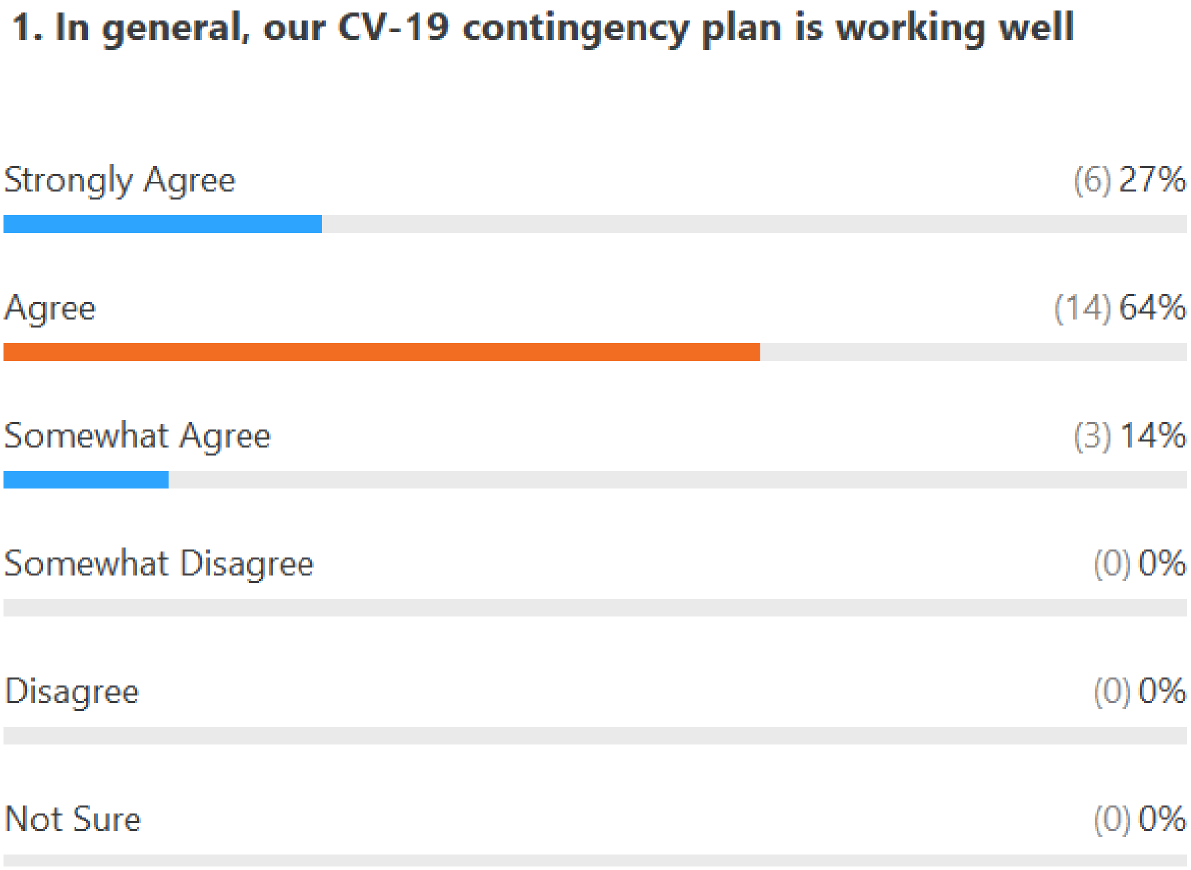
June, you shared a question. What are others doing to keep employees that are not easily changed to remote workers such as workers that are custodians, delivery, etc.? Those kind of out of the IT realm a little bit here.

Another chat talks about keeping track of hours with Active Directory for hourly and audit time cards for VPN.

Paula, you shared when it gets back to keeping track; we have also needed to set management expectations. IT is not the work police and people can be working without being logged in.

Matt A.: Being in trucking we cannot have everybody be remote. There is still that interaction even if it is social distancing with our drivers. So we have a very small footprint of people still at our headquarters which the custodian thing made me think of it. We still have custodians. They still clean the place. It is just that we have sent the majority of the headquarters staff home and so it is all about spreading them out and then the very few that are left there at headquarters, there are still things that require someone to be there to take care of and they are may still be, for example, something being printed. I can print to our headquarters printers. There is stuff on the accounting side. We have spread them out. We have a big operation so we have the majority gone and then those that are left, early on we spread everybody out. So there is still that social distancing. It is just a real challenge in trucking. You can't do 100% everyone not in the facility.

Poll: CV-19 Contingency Plan Working Well



Moderator: Stay safe, strong and positive everyone.

Participant Chat Log:

Arthur Y.: We actually install VPN clients on our desktops and ask our users to bring them home together with their monitor, keyboard and mouse. We weren't able to get any laptops as they were not in-stock.

Chadd B.: We took training laptops we had to send those out. When we ran out of those we started sending desktops home with people.

Clint L.: We did the same thing as Arthur

Greg F.: Moved 30-40 users to loaner laptops with VPN, cranking out Teams

Chadd B.: We send everything home with their desktop. Monitor, keyboard, mouse, etc.

Kevin F.: Yesterday I ordered a few additional laptops from Dell and they have a 35 day delivery time frame. Thankfully they are just to replenish our stock and not critical.

David C.: We ran out of laptops early, can't get more yet, and are allowing and encouraging users to use their personal home systems.

Robert W.: We have been using Chromebooks to supplement

Michael C.: Surprising we were prepared based on standard DR planning for snow storms

Chadd B.: We told people they could use their own headsets/headphones. Most everyone has a pair from a smartphone or their kids had one for them lol

David C.: Robert W., how did the Chromebooks work for you? We use Citrix, and I thought a Chromebook would work well.

David D.: Donnie from DSR has been able to get me computers

Robert W.: We used Office 365 with Forticlient VPN and they are working very well

Greg F.: they can access web based, but limiting VPN to agency devices

Greg Y.: We only allow personal computers with VDI VM Horizon or Citrix with Duo 2-factor

Chadd B.: We are not allowing personal devices

Clint L.: we also require 2-factor when using a personal computer to connect

Donna E.: We started out with designated focus groups such as customer service, financial services, etc.. Personal computers were an option but associates were informed that they had to allow Shaw to install security software on their computer.

Stephen T.: We have everyone working from laptops already so they just got a take them home order

Stephen T.: Home printing and scanning are still issues but mostly for people without large displays at home or who are just mentally stuck in paper land.

Sadie H.: We had to purchase laptops. We were able to purchase some from CDWG.

Jay G.: What will you do with all of the Meraki equipment after this event is over and people move back in the office?

Chadd B.: We are allowing personal printers... not ideal but limited options

Mike O.: Great question!

Chris Z.: Question: For people sending desktops home are you getting a lot of calls on how to plug into the router? Or do they all have wireless cards in desktops?

Anthony D.: I'm here.

Tariq A.: A part of our BC/DR plan about 15 years ago was to replace desktops with laptops and docking stations, this is the first time that plan came into play, we provision VPN for every new employee as onboarding

Sadie H.: We have been following the guidelines from the CDC.
https://www.cdc.gov/coronavirus/2019-ncov/prepare/disinfecting-building-facility.html

Tariq A.: We’ve been using Teams remote control for IT support

Mark M.: devices should be wiped down and quarantined for at least a week

David D.: + 1 for Teams

Chadd B.: Teams +1

Stephen T.: It is — if the printer actually has a disk (happens in the mid-tier and professional models mostly but is poorly documented) then disk disposal rules apply but to the presence of protected data in our world.

Chris Z.: Yeah Teams is working but man there is a lot of sprawl. Governance is a key.

Cory A.: We are pushing users to not print at home. This is forcing paperless for users who have been lazy in adopting digital only workflows. There are some good changes happening due to this business environment.

Sadie H.: We stopped password expiration. For people that change their password remotely. We have them connect to VPN, then lock their computer, then log back in with the new password

Sharon H.: We are scheduling time for the employee to come on site to reset their passwords

Jeff H.: We changed our domain policy to not let passwords expire for the next few months.

Sharon H.: We also extended the password expiration

Michael C.: VPN is the solution

Mark M.: As long as our users are VPN in they can lock their computer and change password from home without issue

Greg E.: NetMotion will allow you to change the password.

Arthur Y.: VPN is the main solution for this, once connected the passwords are synced.

Mark M.: I personally had to do so myself this last week without issue

Tariq A.: We extended our password expiry from 60 days to 90 days, we also use Okta and have some instructions on how to change it online, it eventually trickles down. Also VPN allows them to connect to the domain network to reauthenticate (CTRL-ALT-DEL to change pass through VPN works well)

Cory A.: Azure AD.

Stephen T.: Password changes must be done over VPN — we are in the middle of extending our password policies to match the new NIST guidelines.   At worst it's a lock and unlock screen issue

Chris Z.: Password portal is handy, but that would take time to set up.

Chris M.: Has been a challenge for us as well. We have them connect to VPN and then use Okta to change their password. This is working for us.

Chris Z.: But yes, with VPN password change on laptop changes password in AD which then syncs to O365.

Cory A.: Azure AD connect w/password write back is an option for O365 hybrid users.

Kevin F.: We just let them live with 2 passwords. We are a construction company and it happens all the time with our field teams. It eventually syncs up when they go to a site with a VPN. Some may go 6-9+ months with those 2 passwords. It is just part of being remote but they are used to that.

Chris Z.: If you have MFA I would say you could probably extend password expire for another 3 months.

Arthur Y.: Azure AD password write back only change the password in AD, but not on the laptop. So the passwords are still out-of-sync until VPN is connected.

David D.: +1 Azure AD connect w/password write back is an option for O365 hybrid users

Gilbert I.: in case user cannot change password, the tip to connect his computer is unconnected from Wi-Fi or wired connection, logon to computer then reconnect network

Gilbert I.: in case user cannot change password AND PASSWORD EXPIRED OR ACCOUNT LOCKED, the tip to connect his computer is unconnected from Wi-Fi___33 or wired connection, logon to computer then reconnect network

David D.: The VPN only works if they already have it installed and or the ability to install it.

Mike F.: HIPAA has relaxed

Mike F.: For the reasons of the pandemic

Mike F.: We are doing a lot with EMRs and nursing homes across the country, everyone is understanding the risks are higher.

Robert W.: we were able to not relax any risk. We did have to delay new security steps we were about to roll out.

David C.: Nothing new here.

Paul S.: we are doing a daily report on connected users

Robert W.: tracking who has been send home with suspected COVID19 at our communities

Mike O.: At Olmsted County, we have been keeping track of time which is being used for COVID-19 tasks.

Paul S.: we reached to suppliers to verify support levels

Chris M.: We are telling our suppliers to expect delayed payments

Paul S.: we have been reminding users to be extra cautious and cyber aware while working from home

Donna E.: Some of our facilities contacted the suppliers that they use the most individually.

Cory A.: In terms of associate's time entry - we've modified our in-house time reporting tools to account for FFCRA legislation.

Cory A.: no. home grown

Matt A.: We use Teams

Robert W.: WebEx for us

Steve W.: Teams for us

Edward M.: We are using a product called BlueJeans.

Arthur Y.: I'd like to be able to use Teams Live Event soon, would be good to hear some experiences.

Sadie H.: we use Google Meets

Paul S.: We have been using WebEx mostly, with a planned migrations to MS Teams

Chris Z.: Cisco for us. WebEx. Working pretty well

Matt A.: IT uses Teams; Business uses Zooms

Donna E.: We use google hangouts mostly

Kevin F.: Teams is a lot better than it was 6+ months ago. Teams is working good so far.

David D.: Mostly Teams, sometimes Zoom

Jay G.: We use WebEx and Teams

Chris M.: We use Teams. Looking into Zoom.

Dan L.: Using WebEx. Exploring Teams for cost

Douglas S.: we use adobe connect

Clint L.: We use WebEx as our primary and Teams as our secondary. No Zoom

Gilbert I.: O365 platform

Mike O.: We have found Zoom does not provide HIPAA compliance (without paying $199/month)

Michael C.: WebEx Events when needed, but we are in the conversion to Teams

Mark H.: Primary use WebEx for us

Douglas S.: adobe connect and WebEx

Donna E.: Is anyone concerned about the security issues that have recently come to light in regards to using Zoom?

Mike F.: both Zoom and Teams

Dave G.: Yes Donna ^^^ https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

Stephen T.: Yes.

Michael C.: This morning there was an announcement on Zoom being hacked. Allowing users in meeting who don't belong on the meeting

Chris Z.: Oops.

Stephen T.: The bigger issues are actually the quality and lack of transparency from Zoom about all their security issues.

Greg F.: We are using GoToMeeting for external, Teams actively rolling out for internal

Arthur Y.: I believe the question may be more focused on "Live Events" functionality instead of just video conferencing. So similar to WebEx Webinar function that was just mentioned.

Chris Z.: Just looking at that zoom alert, hopefully everyone is blocking SMB and CIFS from internal to the Internet by default.

Chris Z.: Also have MFA. Really MFA is so nice.

David D.: what about zoom bombing

Chadd B.: Enabled the meeting password

Mike O.: Virtual Coffee breaks

Chadd B.: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-outgoing-ntlm-traffic-to-remote-servers

Chadd B.: That's the GPO fix for the HTML Hash issue

Christopher B.: thank you

Tariq A.: Thanks Chadd very helpful

Tariq A.: We have a twice a day 10 minute group stretching session lead by one of our staff

Sharon H.: I send an email every afternoon with something light hearted.

Chadd B.: Here is the Zoom response

Chadd B.: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Tariq A.: The stretching session is done over Teams video

Chris S.: Virtual Happy Hour has been enjoyable

Chris Z.: Good idea. Only thought it might want to enable audit all first to see what is using NTLM. All sorts of oddball apps can use it and you wouldn't want to break everything.

Chris Z.: I recall doing this a while ago. Took time to get oddballs to Kerberos and Azure/AD.

Chadd B.: Yeah. If you were not auditing before now maybe don't block

Dave G.: Our "treat" has been hot pre-made family meal delivery. One less thing to worry about for working parents.

Chadd B.: We were auditing so we already had the allowed list built

Clint L.: We posted tips and tricks on our corporate intranet related to best practices on connecting remote, troubleshooting your home network, cleaning your PC. We've also been adding content as new remote issues pop up

Donna E.: We had a pandemic response plan in place and our Risk Management & HR teams have done a great job. As for length of time, I was told to work from home until further notice.

Michael C.: And how is everyone measuring user productivity?

Jay G.: We are tracking hours. I'd love to hear more about what others are doing.

Greg F.: struggling with US Mail and it "paper"

Kevin F.: We are anticipating and preparing to do this for another Month. We were 100% cloud to start so that really helped out. So far our Construction sites are still going but in some cases at a slower pace due to changes in how they work at the site. We've had to have more distancing at the sites. Overall, our field crews are adapting well.

Donna E.: We have a weekly activity document that everyone reports on in regards to their job or projects that they may be working on.

David D.: I'm guessing at least another three months and possibly going back to working from home in the fall. I think things have already changed; just people haven't realized it yet

Dave G.: Yes. Forced acceptance. Lack of printing has changed dynamics. Even simple things like print, sign, scan. We capture signatures and now sign within adobe (free).

David D.: yes

Steve W.: We use ManageEngine ServiceDesk, so tickets are monitored

Michael C.: I have been working the task based module. Keeping projects in check and meeting goals of the org.

Mike F.: We are using Toggle to keep hourly people tracking their time.

David D.: You/company have to have set boundaries and expectations

Clint L.: Once this is over, I think we are going to see a lot more people wanting to work from home regularly and it'll be harder for us to say no, you need to be in the office to be effective

Donna E.: At this time and as far as I know, we are to work our regularly scheduled work shift. There are various administrative departments working remotely so I cannot speak to their schedule.

Dave G.: We've been setting user hour limits in Active Directory for hourly. And can audit timecards vs VPN. Definite compliance concerns with hourly employees.

Chadd B.: I think setting hours and sticking to them is key when WFH

Chris Z.: Agreed, this will be a cultural item to add to the company.

Paul S.: we have also needed to set management expectations - IT is not the 'work police', and people can be working without being logged in...

June K.: How are others doing to keep employees that are not easily changed to remote workers? Such as workers that are custodians, delivery...

Jay G.: Any thoughts on CAD users?

Matt L.: Our CAD users are going into the office. RDP sort of works but requires some Local Security Policies changes.

Kevin F.: Autodesk has sent emails to customers with some extended home use options on some projects.

Kevin F.: products.

Kevin R.: We have our CAD users using our VDI as a jump platform to get to their desktops which are still in the office

Kevin F.: Autodesk makes AutoCAD product.

Chadd B.: RDP to a desktop in the office for AutoCAD

Michael C.: Our CAD users are using RDS, and Remote access to onsite desktops

Paul S.: Yes, and we have found that Management has responded well to explanations about what to expect from Remote Access

Greg F.: very good discussion

Gilbert I.: laptops

Chadd B.: Good discussion today

Chadd B.: Stay healthy everyone!

End of discussion

Products/Vendors/Technologies shared in this WebForum:

AutoCAD
CDC
CISCO
Disaster Recovery
FortiClient
GPO
ManageEngine
NetMotion
Okta
RDP
Teams
VPN
Zoom
Azure AD
Chromebooks
Citrix
Duo 2-factor
Google Meets
Kerberos
MS Teams
O365
Passwords
ServiceDesk
VDI VM Horizon
WebEx